WHAT IS CLAIMED IS:

1. A method of displaying data related to an intrusion event on a computer system, comprising:

capturing data related to the intrusion event;

decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans, the decoded data in turn comprising intrusion signature, data summary, and detailed data;

correlating data components of the intrusion signature, data summary and detailed data to one another; and

graphically displaying the correlated decoded data components.

2. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data components comprises graphically highlighting correlated data components of intrusion signature, data summary and detailed data.

3. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data comprises:

receiving a user input selecting a displayed data component;

graphically highlighting data components correlated to the selected data component.

4. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data comprises:

receiving a user input selecting a displayed data component;

graphically highlighting the user selected data component; and

graphically highlighting data components correlated to the selected data component.

5. The method, as set forth in claim 1, wherein capturing data comprises capturing network data packets of the intrusion event.

6. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format.

7. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

8. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

9. The method, as set forth in claim 1, further comprising storing the captured data.

10. A method of graphically displaying data related to an intrusion event on a computer system, comprising:

capturing data related to the intrusion event (the data comprising data components of intrusion signature, data summary, and detailed data);

correlating data components of the intrusion signature, data summary and detailed data to one another; and

graphically displaying the correlated data components.

11. The method, as set forth in claim 10, wherein graphically displaying the correlated data components comprises:

receiving a user input selecting a displayed data component; and

graphically highlighting all data components correlated to the selected data component.

12. The method, as set forth in claim 10, wherein graphically displaying the correlated data components comprises:

receiving a user input selecting a displayed data component;

graphically highlighting the user selected data component; and

graphically highlighting all data components correlated to the selected data component.

13. The method, as set forth in claim 10, wherein capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined signature in the network data packet.

14. The method, as set forth in claim 10, further comprising decoding the captured data from a binary format to a human-readable text format.

15. The method, as set forth in claim 10, further comprising decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

16. The method, as set forth in claim 10, further comprising decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

17. A system of presenting data of an intrusion detection system, comprising:

a network driver capturing data related to an intrusion event upon detecting a predetermined intrusion signature;

a decode engine decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans, the decoded data comprising data components of intrusion event data, data summary, and detailed data; and

a user interface correlating data components of the intrusion signature, intrusion event data, data summary and detailed data to one another and displaying the correlated decoded data components.

18. The system, as set forth in claim 17, wherein the user interface graphically highlights correlated data components of intrusion event data, data summary and detailed data.

19. The system, as set forth in claim 17, wherein the user interface is operable to receive a user input selecting a displayed data component, and graphically highlight all data components correlated to the selected data component.

20. The system, as set forth in claim 17, wherein the user interface is operable to receive a user input selecting a displayed data component, highlight the user selected data component, and highlight all data components correlated to the selected data component.

21. The system, as set forth in claim 17, wherein the network driver captures network data packets of the intrusion event in response to the intrusion detection system detecting a predetermined intrusion signature.

22. The system, as set forth in claim 17, wherein the decode engine decodes the captured data from a binary format to a human-readable text format.

23. The system, as set forth in claim 17, wherein the decode engine decodes the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

24. The system, as set forth in claim 17, wherein the decode engine decodes the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.